

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
FORT MYERS DIVISION

UNITED STATES OF AMERICA

v.

CASE NO.: 2:22-cr-53-SPC-NPM

RICHARD EDWARD BRILLHART

---

**OPINION AND ORDER<sup>1</sup>**

Before the Court is Defendant Richard Brillhart's Motion to Suppress ([Doc. 56](#)), along with the Government's opposition ([Doc. 57](#)). The Court held an evidentiary hearing, which Defendant attended with counsel. ([Doc. 70](#)). The Court reserved ruling at the hearing's conclusion but now issues this decision to explain why it denies the Motion.

**BACKGROUND**

This case is about child pornography—distribution and possession. ([Doc. 1](#)). And Defendant's motion is about how law enforcement discovered the contraband. The short story is Defendant allegedly emailed hundreds of child pornography images and videos through his Yahoo and Google accounts and uploaded files to Google Photos. Defendant did so all within about a one month

---

<sup>1</sup> Disclaimer: Papers hyperlinked to CM/ECF may be subject to PACER fees. By using hyperlinks, the Court does not endorse, recommend, approve, or guarantee any third parties or their services or products, nor does it have any agreements with them. The Court is not responsible for a hyperlink's functionality, and a failed hyperlink does not affect this Order.

span.<sup>2</sup> When Yahoo and Google discovered Defendant's conduct, they notified the National Center for Missing and Exploited Children (NCMEC), which is a clearinghouse for electronic service providers to report child sexual abuse material. Yahoo and Google also attached the offending files. NCMEC then forwarded the files to law enforcement, who viewed them without a warrant. Based on what they saw and further investigation, law enforcement secured search warrants, the evidence from which led to Defendant being indicted for child pornography offenses.

Defendant now seeks the Fourth Amendment's protection. He moves to suppress all evidence against him because law enforcement performed an unlawful search by viewing the images and videos from Yahoo and Google without a warrant. At the hearing, the Government introduced twenty-one exhibits and called three witnesses: (1) Jordyn Kramer, a Yahoo custodian of records and investigator on its E-Crimes Investigation Team; (2) Anjali Shrestha, a Google custodian of records and team lead for its Legal Investigations Support team; and (3) Katrina Lee, a South Florida Internet Crimes Against Children Task Force Officer ("TFO Lee").<sup>3</sup> (Doc. 70-1).

---

<sup>2</sup> This all allegedly occurred approximately five months of Defendant being released from federal prison for possessing child pornography. *See United States v. Brillhart*, No. 2:03-cr-121-JES-121 (M.D. Fla. 2006) (sentencing Defendant to 240 months' imprisonment for possession of materials involving the sexual exploitation of minors in violation of [18 U.S.C. §§ 2252\(a\)\(4\)\(B\)](#) and [2252\(b\)\(2\)](#)).

<sup>3</sup> TFO Lee's last name was O'Brien during the relevant parts of the investigation.

Defendant introduced three exhibits but offered no witnesses. (Doc. 70-23). The relevant facts are not in dispute. Even so, the Court makes these factual findings material to the Motion based on the evidence presented:

Between April 15 and May 25, 2021,<sup>4</sup> Yahoo and Google filed seven cybertips to NCMEC about child pornography found on Defendant's accounts. Their information led to NCMEC generating nine CyberTipline Reports: four reports and two supplements based on Defendant's Yahoo activity, and three reports based on his Google activity. Information from Yahoo and Google common in all the Reports included details on the

- user names provided when he registered the accounts, a birthday, mobile phone numbers, email addresses, and IP addresses
- MD5 hash values,<sup>5</sup> and where the files were located (e.g., email attachments)
- emails the user exchanged with the child pornography, including dates and times, sent and received, and attachments

(Doc. 70-2 to Doc. 70-10).

Aside from Yahoo's and Google's information, NCMEC added its own material to the Reports. For example, NCMEC pinpointed Defendant's

---

<sup>4</sup> Unless otherwise indicated, all dates in this Opinion and Order occurred in 2021.

<sup>5</sup> A hash value is a unique string of letters and numbers that reflects the content of an image or video file and is created using a common algorithm like MD5. The series of letters and numbers are a file's digital fingerprint. Generally, electronic service providers assign a hash value to a known child pornography image or video. They scan a designated repository for files with the same value. When they get a "match," they know the scanned file is a duplicate of the child pornography without needing to open or view the file.

approximate geolocation running the IP addresses that Yahoo and Google gave through “a publicly-available online query.” NCMEC also used “publicly-available, open-source websites” to identify Defendant as a registered sex offender, and it named other related CyberTipline reports. Now for specifics on each report.

**a. Yahoo CyberTipline Report 89005640 and Supplemental Report 89347533**

On April 15, Yahoo alerted NCMEC about six child pornographic images, which led to CyberTipline Report 89005640. (Doc. 70-2). Yahoo identified “richard bri” as the suspect who sent six emails through its platform, each of which attached an image categorized as “A1.”<sup>6</sup> A Yahoo employee viewed each image to confirm its content before sending them to NCMEC. Upon receiving the information, an NCMEC staff member viewed one file. NCMEC also used its hash tag technology to confirm all the images were child pornography.

On April 23, Yahoo submitted a supplemental report to NCMEC that said more about Defendant and the images:

The Yahoo accounts jobs4rich@yahoo.com reported for sharing [child sexual abuse imagery (“CSAI”)] using Yahoo Mail, as observed in CyberTip 89005640. The

---

<sup>6</sup> The A1 label is based on an industry classification system that electronic service providers use to identify content in illicit material. A1 means content showing a prepubescent minor engaging in a sex act. A “sex act” is defined as “[a]ny image of sexually explicit conduct (actual or simulated sexual intercourse genital-genital, oral-genital, anal-genital, or oral-anal whether between persons of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.” (Doc. 70-2).

CSAI reported in this CyberTip includes approximately 6 images of nude prepubescent female children, some of whom are engaged in sexual acts with adult males.

Based on the login records and subscriber information for the user's Yahoo account along with open source research, the user appears to be an individual named Richard Edward Brillhart III (BRILLHART), residing in or around Fort Myers, Florida. A further investigation by the Verizon Media E-Crimes Investigations Team (VM-ECIT) has revealed that Brillhart appears to be a Registered Sex Offender in Florida for a prior sex crime conviction involving a child (committed in Michigan).

(Doc. 70-6). It also provided two IP addresses "located in or around Fort Myers, Florida" for "recent successful logins" from the Yahoo account. (Doc. 70-6 at 4). Finally, it provided an address for Defendant: 5446 Tenth Avenue in Fort Myers, Florida 33907.

#### **b. Yahoo CyberTipline Report 90109206**

Yahoo provided a second Cybertip on May 12 that led to Report 90109206. (Doc. 70-3). This time, Defendant operated under the account name "REB REB" and used the email address reb3280@@yahoo.com to exchange about two dozen emails with 271 videos and images attached. A Yahoo employee viewed each file to confirm the child pornography content before sending them to NCMEC. Many files were also designated as A1 material.

When NCMEC received the report, a staff member viewed twenty-two files to confirm the child pornography and the other images were run through its hash tag technology.

**c. Yahoo CyberTipline Report 90418734**

On May 17, Yahoo again contacted NCMEC about more emails involving child pornography that Defendant exchanged. (Doc. 70-4). According to the report, reb3280e@yahoo.com exchanged four emails with ten attached videos with another user. For each video, a Yahoo employee viewed the entire content to confirm child pornography, four of which included A1 material. NCMEC staff later viewed three of the ten videos and submitted the CyberTipline Report to law enforcement.

**d. Yahoo CyberTipline Report 90572327**

On May 19, Yahoo submitted a fourth cybertip about Defendant's child pornography. (Doc. 70-5). It uploaded eight files—seven of them categorized as A1—from emails involving “yngluv01@yahoo.com.” Although the email address changed,<sup>7</sup> Defendant's registered name of “Reb Reb” and verified mobile phone number did not. (Doc. 70-5 at 5). The report again confirmed

---

<sup>7</sup> Kramer testified that Yahoo deactivates an account that's no longer accessible to a user after child pornography is confirmed and a CyberTipline is reported. Yahoo, however, does not prevent the same user from opening a new account under a different name and email address.

that a Yahoo employee viewed the entire content of each file to confirm it was child pornography. An NCMEC staff later viewed five videos.

**e. Yahoo Supplemental Report 91186992**

On May 25, Yahoo submitted a second supplemental report that linked to three CyberTipline Reports. (Doc. 70-7 at 7). It again named Defendant as the suspect and listed the same address, mobile number, and birthday. Yahoo also confirmed Defendant's status as a registered sex offender and added that he had "been recently released from Federal Prison following a 240 month sentence for the sexual exploitation of minors." (Doc. 70-7 at 1). The supplemental report expanded on the images and videos: "nude female and partially clothed female children, ranging in age from approximately toddler to preteen, many of whom are engaged in sexual acts with adult males." (Doc. 70-7 at 4-5). Finally, it provided the IP addresses for recent successful logins to the Yahoo accounts to be in south Florida.

**f. Google CyberTipline Report 90034851**

On May 10, Google submitted a Cybertip about two images stored on its Gmail platform. (Doc. 70-8). Google's information led to NCMEC submitting CyberTipline Report 90034851, which identified the suspect as "Reb Reb" at reb3280@gmail.com. For the first file, someone at Google viewed all the content and categorized it as B1 material "concurrently to or immediately

preceding the sending of the CyberTip.” (Doc. 70-8 at 3).<sup>8</sup> Although Google did not open the second file concurrently with sending its cybertip, an individual at some point earlier reviewed it and matched the hash value of the reported image to determine it contained child pornography. (Doc. 70-8 at 3). When NCMEC received Google’s information, it too matched both files to hash values in its repository for child pornography content.

#### **g. CyberTipline Report 90533145**

On May 19, NCMEC received a second report from Google about one file stored on Google Photos for “Reb Reb” at the verified email address of reb3280e@gmail.com. (Doc. 70-9). For this file, a B1 designation, someone for Google viewed it to “confirm that it contained apparent child pornography concurrently to or immediately preceding the sending of the CyberTip.” Although NCMEC did not view the file, it had a hash match.

#### **h. Google CyberTipline Report 91101569**

On May 25, Google submitted a third report of child pornography and uploaded one video stored in Google Photos. (Doc. 70-10). Again, the suspect was “Reb Reb” at the verified email address of luvemyng04@gmail.com. Google categorized the video as B1. And it was able to do so because “[a] person at

---

<sup>8</sup> A B1 designation is part of the same industry classification system that electronic service providers use to identify content in illicit material. B1 means content showing a pubescent minor engaging in a sex act.



Google viewed the file to the extent necessary to confirm that it contained apparent child pornography concurrently to or immediately preceding the sending of the CyberTip.” (Doc. 70-10 at 3). For NCMEC, it had a hash match of the video.

All nine CyberTipline Reports and Supplemental Reports eventually landed on TFO Lee’s desk. Upon receiving them, she focused on the files that Yahoo and Google uploaded because she knew that someone at the companies had (at some point) viewed the files to confirm they contained child pornography. And for the files with the A1 and B1 categorization, she knew they depicted prepubescent and pubescent minors engaging in sex acts. So TFO Lee opened the files to verify their contents. Based on TFO Lee’s review, law enforcement got search warrants for Defendant’s Yahoo accounts, Google accounts, home, and car. (Doc. 70-11; Doc. 70-12; Doc. 70-13; Doc. 70-14). These searches led to the Indictment and Defendant’s motion to suppress.

## **DISCUSSION**

Defendant argues the Court should exclude all evidence against him because TFO Lee violated his Fourth Amendment rights when she viewed the images and videos without a warrant. From there, he asserts the private search doctrine does not save the warrantless search for two reasons. First, because the names of Yahoo’s and Google’s employees who viewed the files are unknown, the Court only has hearsay evidence that somebody viewed the files,

which does not satisfy his Sixth Amendment confrontation rights. Second, Defendant argues that NCMEC is a government entity who exceeded Yahoo's and Google's searches because they processed the photos through their hash tag repositories and investigated IP addresses for geolocations.

For its part, the Government maintains that Defendant "frustrated or eliminated his expectation of privacy by uploading and sending child pornography over Yahoo and Google, which are private companies that routinely report to NCMEC when they become aware that a customer is sending child pornography using their products or services." ([Doc. 57 at 20](#)). It also argues that TFO Lee replicated Yahoo's and Google's private searches, so the Fourth Amendment did not require her to secure any warrant before viewing the reported images and videos. Finally, the Government raises the good-faith exception to the exclusionary rule.

The Court will address all arguments, starting with the private search exception to the warrant requirement.

### **A. Private Search Doctrine**

The Fourth Amendment protects individuals against the government performing unreasonable searches and seizures. [U.S. Const. amend. IV](#). The government usually needs a warrant before it may search a person or his effects. A warrantless search is thus invalid unless an exception applies to the

warrant requirement. See *Katz v. United States*, 389 U.S. 347, 357 (1967). The exception the Government relies on is the private search doctrine.

The Fourth Amendment protects individuals from government actors, not private ones. A private party may thus conduct a search that would be unconstitutional if the government did it. From this principle comes the private search doctrine. When a private party acts on its own accord and provides evidence against a defendant to the government, the police need not “avert their eyes.” *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971). So the Fourth Amendment lets police replicate a past private search provided it stays within the same parameters. See *United States v. Sparks*, 806 F.3d 1323, 1334 (11th Cir. 2015) (“So once an individual’s expectation of privacy in particular information has been frustrated by a private individual, the Fourth Amendment does not prohibit law enforcement’s subsequent use of that information, even if obtained without a warrant.” (citations omitted)), *overruled on other grounds by United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020).

The Supreme Court formalized the private search doctrine decades ago in two cases: *Walter v. United States*, 447 U.S. 649 (1980)<sup>9</sup> and *United States*

---

<sup>9</sup> In *Walters*, the Supreme Court concluded that FBI agents exceeded the scope of a private search by corporate employees who opened packages that contained boxes of eight-millimeter films “depicting homosexual activities,” because the agents had to watch the films—when no employee had done so—to know whether the defendants committed any crime. 447 U.S. at 649-54, 657 (1980).

*v. Jacobsen*, 466 U.S. 109, 120 (1984).<sup>10</sup> Both considered a warrantless government search after a private party gave the government information for its investigation. Together, the cases determined that a past private search excuses the government from getting a warrant to repeat the search but only when the government's search does not exceed the scope of the private one.

Here, it is undisputed that Yahoo and Google are private entities that acted independently of law enforcement and without the government's knowledge or participation in discovering the child pornography files. Still, Defendant makes much ado about not knowing the identities of the individuals at Yahoo and Google who viewed the files. Without names, Defendant asserts Yahoo's and Google's custodians only offer hearsay evidence about the human review, which violates his right to confront those individuals. But this argument misses the mark for two basic reasons. First, Yahoo and Google, along with their employees and contractors are private people. So the who and how those private companies search their programs does not lessen the private search doctrine's application here. See *United States v. Montijo*, No. 2:21-cr-75-SPC-NPM, 2022 WL 93535, at \*5 (M.D. Fla. Jan. 10, 2022); see also *United*

---

<sup>10</sup> In *Jacobsen*, the Supreme Court concluded DEA agents did not exceed the scope of a private search by Federal Express employees who opened a damaged package with a tube holding zip-lock bags of a white powder, because (1) the agents gleaned no new information than what the employees told; and (2) "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of the private conduct." 466 U.S. at 120-21, 126 (1984).

*States v. Bonds*, No. 521CR00043KDBDCK, 2021 WL 4782270, at \*4 (W.D.N.C. Oct. 13, 2021) (rejecting the defendant’s argument that the anonymous Google employee was unreliable because law enforcement could not contemporaneously verify the information before conducting its search).

Second, the Court can rely on hearsay and other evidence at a suppression hearing that may not otherwise be admissible. *United States v. Raddatz*, 447 U.S. 667, 679 (1980) (“At a suppression hearing, the court may rely on hearsay and other evidence, even though that evidence would not be admissible at trial.”); *see also* Fed. R. Evid. 104(a), 1101(d)(1).

Having settled that, the Court turns to whether the private search doctrine applies here. To start, the Court finds that Kramer and Shrestha testified credibly about Yahoo’s and Google’s internal procedures for identifying, confirming, and reporting child pornography material. They clarified that Yahoo and Google screen for child pornography, not at the direction of law enforcement, but for their own reasons—to protect their brands, reputations, and services from harmful content. Kramer and Shrestha both confirmed that Yahoo and Google followed their procedures when assessing Defendant’s files. Defendant offers no evidence that the CyberTipline Reports, nor Kramer’s and Shrestha’s testimony does not mean what they say: Yahoo and Google reviewed the contents of the actual files, and not just the associated hash tags, before the file was forwarded to NCMEC,

and then to law enforcement. *See, e.g., United States v. Bohannon*, No. 19-CR-00039-CRB-1, 2023 WL 2347420, at \*1 (N.D. Cal. Mar. 2, 2023) (finding a Microsoft employee viewed the contents of the defendant’s OneDrive file before forwarding it to NCMEC).

Moving on, law enforcement did not exceed the scope of Yahoo’s or Google’s searches because TFO Lee only viewed the images and videos they provided. When TFO Lee viewed Defendant’s files, she knew they would contain child pornography and that many would show A1 and B1 content. Defendant makes no argument—nor does the Court see how one can be made—that TFO Lee learned more from viewing the files than Yahoo and Google provided. Because individuals for Yahoo and Google reviewed the files before they were forwarded to NCMEC, who confirmed they were child pornography, TFO Lee did not need to view them to know Defendant committed a federal crime. Yahoo and Google already told her so with the A1 and B1 labels. *See generally Rogers v. Sec’y, Dep’t of Corr.*, No. 8:17-CV-2680-T-33SPF, 2019 WL 2646544, at \*6 (M.D. Fla. June 27, 2019) (finding a § 2255 petitioner did not “identif[y] any clearly established federal law holding that when a private searcher views at least one image on a disk and tells police that the disk contains contraband, police exceed the scope of the private search by viewing other images on that same disk”), *aff’d*, 829 F. App’x 437 (11th Cir. 2020).

So this not a case where a private citizen stumbled across child pornography on a laptop and gave the device to law enforcement who then searched the device's entire contents. Rather, individuals at Yahoo and Google, who are trained on what constitutes child pornography under federal law, verified the illicit content on the files. And because TFO Lee only viewed the files that Yahoo and Google provided, she got the same information discovered during the private search. Under these facts, TFO Lee did not need to avert her eyes from the videos and images when she received the CyberTipline Reports. [\*Coolidge\*, 403 U.S. at 489](#).

Finally, as much as Defendant argues that NCMEC is a governmental agency that expanded on Yahoo's and Google's private searches because it searched for geolocations, his argument misses the mark. Yahoo and Google gave NCMEC several IP addresses for the suspect, and from there, NCMEC investigated more through open sources. Even so, it is well established that law enforcement need not get a search warrant to investigate an IP address. [\*See United States v. Ryan Anthony Adams\*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at \\*3 \(M.D. Fla. Aug. 10, 2016\)](#) ("Computer users lack a legitimate expectation of privacy in information regarding the to and from addresses for emails, the IP addresses of websites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user."

(citations omitted)); *see also* [United States v. Solove](#), No. 21-11747, 2022 WL 152240, at \*1 (11th Cir. Jan. 18, 2022) (holding the *Carpenter* exception to the third-party doctrine does not extend to email and IP addresses). What's more, Yahoo provided Defendant's home address in its first supplemental report based on its own investigation. And, in the end, the search warrant for Defendant's home is that same address from Yahoo. *Compare* Doc. 70-6 at 4, *with* Doc. 70-13 at 53. So neither NCMEC nor law enforcement needed to do any additional search—Yahoo did it for them.

In conclusion, the Court finds the private search doctrine applies to justify the warrantless search of the videos and images uploaded to the CyberTipline Reports.

## **B. Reasonable Expectation of Privacy**

The Court further finds that Defendant did not have a reasonable expectation of privacy in the videos and images he uploaded to Yahoo's and Google's platforms. And Defendant neither presents evidence nor argues to the contrary.

A defendant can only invoke the Fourth Amendment's protection where he has a legitimate expectation of privacy in the item searched. *See Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978). The privacy interest is both subjective and objective: a defendant must show he subjectively expected privacy, and the expectation is one that society recognizes as reasonable. *See United States v.*



*Ford*, 34 F.3d 992, 995 (11th Cir. 1994) (citation omitted). But an individual's expectation of privacy is not always forever. A common example of when an expectation of privacy is frustrated is when information is revealed to a third party. See *Jacobsen*, 466 U.S. at 117 ("It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information[.]" (citation and footnote omitted)).

Defendant revealed the videos and images not only to his intended email recipients, but also to Yahoo and Google. He risked that both would turn them over to the Government. And the Court need look no further than Yahoo's and Google's written policies to know it gave Defendant fair warning of that risk.

Yahoo posts a Transparency Report on its website that tells users how it uses automated scanning technologies and human review to detect unlawful child pornography on its platforms. (Doc. 70-17). From there, Yahoo advises how its team of human reviewers evaluate detected images to confirm the content as child pornography. It is also clear that Yahoo reports all child pornography to NCMEC and includes subscriber information on who uploaded the files.

Yahoo’s Transparency Report isn’t the only place where Yahoo shares how it spots and reports child pornography. Its Terms of Service echo the procedure: “You agree not to use the Services to: . . . make available any content that is harmful to children, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another’s privacy, hateful, or racially, ethnically, or otherwise objectionable[.]” (Doc. 70-15 at 2; Doc. 70-16 at 3)). A user also agrees not to use Yahoo’s service to “violate any applicable laws or regulations.” (Doc. 70-15 at 2; Doc. 70-16 at 3).

Like Yahoo, Google openly tells its users about its quest to find, review, and report child pornographic material on its platforms through its Transparency Report and Terms of Service. (Doc. 70-18; Doc. 70-20). According to Google’s Transparency Report, its “teams work around the clock to identify, remove, and report this . . . content, using a combination of industry leading automated detection tools and specifically trained reviewers. We also receive reports from third parties and our users, which complement our ongoing work. We report [child pornography] to the National Center for Missing and Exploited Children, NMEC, . . . [who] may send those reports to law enforcement agencies around the world.” (Doc. 70-20). Under Google’s Terms of Services (Doc. 70-18), a user agrees to follow the laws and not abuse or harm others. Users are also advised that Google employs automated

systems to check for child pornography sent, received, and stored on its platform.

And Yahoo and Google are not all words without action. They both told their users that they follow through on their internal procedures. For example, in 2021, Yahoo reported 5,498 accounts to NCMEC for trafficking in child pornography on its platforms and filed 341 supplemental reports with NCMEC. Also in 2021, Google submitted over 850,000 CyberTipline reports to NCMEC. (Doc. 70-20; Doc. 70-21).

Because of the Terms of Service and Transparency Reports, Yahoo and Google warned Defendant he risked being reported to law enforcement or NCMEC if either discovered that he sent, received, or distributed apparent child pornography. Even if Defendant believed that his emails and photos were private, society is not prepared to recognize that belief as reasonable given the Terms of Service and Transparency Reports. In the end, Defendant lost any expectation of privacy in the files once he hit send. *See United States v. Odoni*, 782 F.3d 1226, 1238 (11th Cir. 2015) (“An individual does not have a reasonable expectation of privacy in an object to the extent the object has been searched by a private party.” (citation omitted)). Without a reasonable expectation of privacy, TFO Lee did not violate Defendant’s Fourth Amendment rights when she viewed the files, and any privacy was waived by Yahoo’s and Google’s prior searches.

### C. Good-faith exception

Even if Defendant had a reasonable expectation of privacy and the private search doctrine did not apply, the Court still denies the Motion under the good-faith exception. To discourage police from violating the Fourth Amendment, courts have created the remedy of excluding “improperly obtained evidence at trial.” *Herring v. United States*, 555 U.S. 135, 139 (2009). But “exclusion ‘has always been our last resort, not our first impulse.’” *Id.* at 140 (citation omitted). The exclusionary rule’s “sole purpose . . . is to deter future Fourth Amendment violations.” *Davis v. United States*, 564 U.S. 229, 236-37 (2011) (citations omitted).

Courts must thus engage in a “rigorous weighing of [exclusion’s] costs and deterrence benefits” to determine whether it is needed. *Id.* at 238. And the good-faith exception comes into that analysis. Under the exception, courts do not exclude evidence when law enforcement acts, as here, in “objectively reasonable reliance upon a statute authorizing” the search. *Illinois v. Krull*, 480 U.S. 340, 349 (1987) (“The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer’s actions as would

the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant.”).

TFO Lee acted in objectively reasonable reliance on Yahoo’s and Google’s statutory reporting requirements to view the files here. *See* [18 U.S.C. § 2258A](#); *see also United States v. Ackerman*, 804 F. App’x 900, 905 (10th Cir. 2020) (finding the good-faith exception applied when NCMEC searched the defendant’s email in good faith under § 2258A). Electronic service providers like Yahoo and Google must report to NCMEC’s CyberTipline after it obtains “actual knowledge” of any apparent child pornography. [18 U.S.C. § 2258A\(a\)\(1\)-\(2\)](#). They can even be fined if they do not do so. *Id.* [§ 2258A\(c\)](#). NCMEC too has statutory obligations. It must maintain the CyberTipline and forward every report it receives to law enforcement. *Id.* [§ 2258A\(a\)\(1\)\(B\) & \(c\)](#). Congress has also let NCMEC receive and review the illicit material without breaking the law. *Id.* [§ 2258A\(c\)](#).


Under this statutory scheme, TFO Lee acted in reasonable reliance on Yahoo’s, Google’s, and NCMEC’s legal obligations to view the files she received. *See generally United States v. Leon*, 468 U.S. 897, 918 (1984) (stating the exclusion of evidence is an “extreme sanction” that “should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule”). The Court thus denies Defendant’s Motion on the good-faith exception too.

Accordingly, it is now

**ORDERED:**

Defendant Richard Brillhart's Motion to Suppress ([Doc. 56](#)) is **DENIED**.

**DONE AND ORDERED** in Fort Myers, Florida on May 7, 2023.

  
**SHERI POLSTER CHAPPELL**  
**UNITED STATES DISTRICT JUDGE**

Copies: Counsel of Record